

Excerpt from
Japanese Utility Model Laid-Open Publication No. Sho 56-156134

The present invention will be described by means of an embodiment.

Fig. 1 is a block diagram showing one embodiment of the present invention.

Numerals 1, 2, 3, 4, and 5 denote a general logical random number generating circuit which is conventionally used; numeral 2 denotes a natural random number generating circuit which picks up noises occurring in nature, such as a thermal noise and a radiation noise, and outputs the noises after applying wave shaping thereto; numeral 3 denotes a half-adder; numeral 4 denotes a readable/writable memory circuit for storing the output from the half-adder 3; and numeral 5 denotes a control circuit which supplies an output to the logical random number generating circuit 1, the natural random number generating circuit 2, and the half-adder 3 to instruct to extract outputs from the logical random number generating circuit 1 and the natural random number generating circuit 2 at matched timing and synthesize the outputs in the half-adder 3 for outputting to the memory circuit 4 where only the necessary bit numbers are stored.

Here, the natural random number generating circuit 2 is configured as shown in Fig. 2, for example.

Specifically, numeral 6 denotes a Zener diode, and a thermal noise from the Zener diode 6 is amplified in an amplifier 7. An output from the amplifier 7 is subjected to wave shaping in a Schmitt circuit 8 whose output is then input, as a clock pulse, to a D flip flop 9. An output from the D flip flop 9 is supplied to a shift register, which is not shown, and is extracted from the shift register at the output timing from the control circuit 5.

Then, the output from the logical random number generator 1 and the output from the natural random number generating circuit 2 are added by the half adder 3. The added value is stored

in the memory circuit 4 for used in encryption of communication message.

Further, assuming that binary decimal numbers are used, for example, from the values output from the half adder 3 which are stored in the memory circuit 4, output values corresponding to decimal numbers 10 to 15 are discarded when they are output from the memory circuit 4 and new outputs are taken from the half adder 4, whereas output values corresponding to decimal numbers 0 to 9 are output as one numeral value of a random number sequence.

While in the above example, a single pair of the logical random number generating circuit 1 and the natural random number generating circuit 2 is used, a plurality of pairs may be used and synthesized.

According to the present invention, because the output from the natural random number generating circuit and the output from the logical random number generating circuit are calculated, the problem caused when only the logical random number generating circuit is used can be solved. Further, when only the natural random number generating circuit is used, the random numbers principally have no periodicity, there is still a possibility that the frequency of occurrence of output value becomes uneven during a short period.

However, this defect caused by the natural generating circuit is also solved because the output from the logical random number generating circuit is calculated with the output from the natural random number generating circuit.

Accordingly, the present invention is very effective when used in a code converting circuit for encoding a signal or the like in a code communication system or the like, to provide an effect which makes decoding difficult.

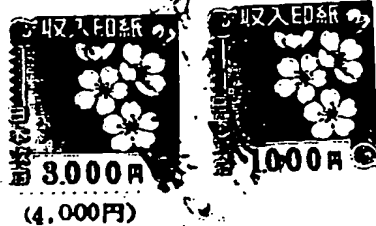
4. Brief Description of Drawings

Fig. 1 is a block diagram of one embodiment of the present invention; and

Fig. 2 is a circuit diagram of an example natural generating

circuit which is used in one embodiment of the present invention.

1: logical random number generating circuit, 2: natural random number generating circuit, 3: half adder, 4: memory circuit, 5: control circuit



実用新案登録願

昭和55年4月2/日

特許庁長官 川原能雄 殿

1. 考案の名称

ランスウハツセイカイロ
乱数発生回路

2. 考案者

住所 ミナトクシシロガネ
東京都港区芝白金6-16-42
氏名 ミヤノ マサヨシ
官野正義

3. 実用新案登録出願人

住所 ヨコハマシコウホクフトオチヨウ
神奈川県横浜市港北区太尾町910番地
名称 デンシ
ニコー電子株式会社
代表者 サクラ イ シゲ キ
桜井茂樹

4. 代理人 〒166

住所 東京都杉並区高円寺南一丁目29番16号 TEL. 382-6771(代)
氏名 弁理士 (5654) 渡辺軍治

5. 添付書類の目録

(1) ✓ 明細書
(2) ✓ 図面

1 通 (3) ✓ 委任状
1 通 願書の副本

1 通
1 通

式査 (5R)

特許庁 (5)
55.4.22
出願第二課

✓ 55 054192

156134

明 細 書

1. 考案の名称

乱数発生回路

2. 実用新案登録請求の範囲

論理乱数発生回路と、自然乱数発生回路と、論理乱数発生回路の出力と自然乱数発生回路の出力とを論理演算する演算回路とを備え、演算回路の出力を乱数出力とすることを特徴とする乱数発生回路。

3. 考案の詳細な説明

本考案は暗号通信系などにおける信号を暗号化する符号変換器などに使用できる乱数発生回路に関する。

従来、前記符号変換器などに使用される乱数発生回路は論理乱数を発生する。論理乱数は予めその発生数列を予測することができ、復元性があるために符号変換器などに使用される。逆に言えば論理乱数は周期性を必然的に有するものであり、論理乱数で通信文を暗号化した場合、解読の可能性が存することになる。

本考案は周期性を無くした乱数を発生する乱数発生回路を提供することを目的とし、この目的は論理乱数発生回路と、自然界に存在する雑音をピックアップしかつ波形整形して出力とする自然乱数発生回路と、論理乱数発生回路の出力と自然乱数発生回路の出力とを論理演算する演算回路とを備え、演算回路の出力を乱数列として用いることにより達成される。

以下、本考案を実施例により説明する。

第1図は本考案の一実施例のブロック図である。

1は従来から用いられている通常の論理乱数発生回路であり、2は自然界に存在する雑音、たとえば熱雑音、放射線雑音などをピックアップして波形整形して出力とする自然乱数発生回路であり、3は半加算器であり、4は半加算器3の出力を記憶する読み書き可能な記憶回路であり、5は論理乱数発生回路1、自然乱数発生回路2、半加算器3に出力してタイミングを合せて論理乱数発生回路1、自然乱数発生回路2からの出力を取り出し、半加算器3にて合成して記憶回路4へ出力して必

要ビット数だけ記憶回路 4 に記憶することを指令する制御回路である。

ここで自然乱数発生回路 2 はたとえば第 2 図に示す如く構成されている。

すなわち、6 はツエナーダイオードであり、ツエナーダイオード 6 からの熱雑音を増幅器 7 で増幅し、増幅器 7 の出力はシュミット回路 8 で波形整し、シュミット回路 8 の出力を D フリップフロップ 9 にクロックパルスとして入力し、D フリップフロップ 9 の出力を図示しないシフトレジスタに入力し、シフトレジスタから制御回路 5 からの出力タイミングで取り出すように構成してある。

そこで論理乱数発生器 1 からの出力は自然乱数発生回路 2 からの出力は半加算器 3 で加算され、この加算値は記憶回路 4 に記憶され、たとえば通信文の暗号化に使用する。

また、たとえば 2 進化 10 進数を利用するものとするれば記憶回路 4 に記憶した半加算器 3 からの出力中、10 進数 10 ~ 15 に対応する場合には記憶回路 4 からの出力時これを廃棄して新たに半加算

器 3 からの出力を取り入れ、10進数 0～9 に対応する場合にはこれを乱数列の一つの数値として送出するようにする。

以上は論理乱数発生回路 1 および自然乱数発生回路 2 が 1 組の場合の例について説明したが複数組を用いて合成してもよい。

そこで本考案によれば論理乱数発生回路のみによるときは前記した如き問題があるが、自然乱数発生回路の出力と論理乱数発生回路の出力とを演算したために論理乱数発生回路のみの場合の問題を解決し得る。また、自然乱数発生回路のみの場合は周期性は原則的には無いが、短期間においては出力値の発生頻度が片寄る可能性を有している。

しかし、これに論理乱数発生回路が演算されるため自然発生回路の上記欠点も解消される。

従つて、本考案によれば暗号通信系などにおける信号を暗号化する符号変換回路などに使用してきわめて有効で解読が困難となる効果もある。

4. 図面の簡単な説明

第 1 図は本考案の一実施例のブロック図。

第 2 図は本考案の一実施例に用いる自然発生回路の一例の回路図。

1 : 論理乱数発生回路, 2 : 自然乱数発生回路,
3 : 半加算器, 4 : 記憶回路, 5 : 制御回路。

考案者 宮 野 正 義

出願人 ニ コ ー 電 子 株 式 会 社
代表者 桜 井 茂 樹

代理人 弁理士 渡 辺 軍 治

図1

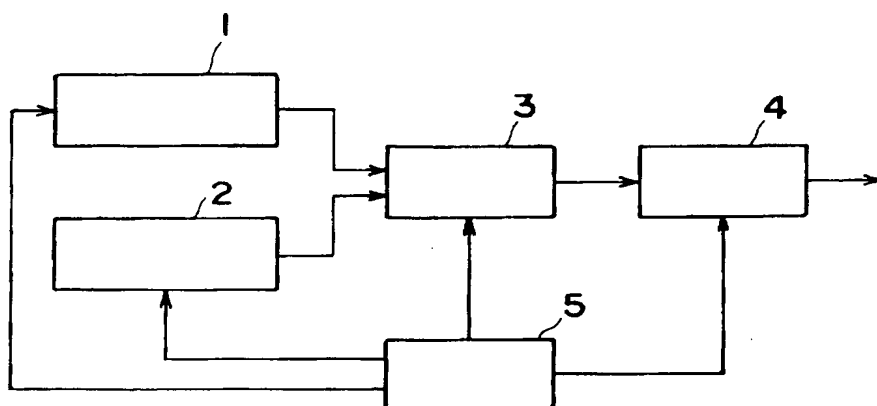
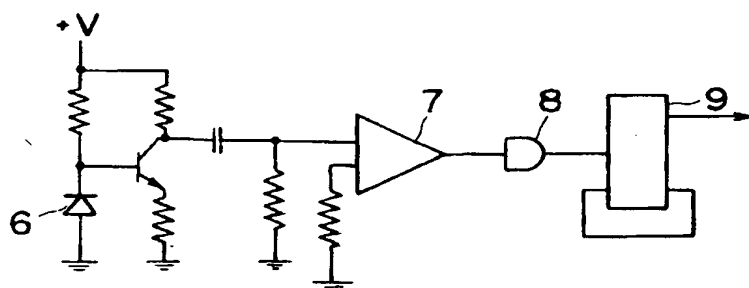


図2



出願人 ニコ電子株式会社

代理人 弁護士渡辺重治

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.